DOWNLOADING OF DATA TO SECURE DEVICES

BACKGROUND

Content access transmission and communication systems, e.g., high speed data, audio and video content transmission systems, serve numerous users where each user has one or more devices (e.g., display devices, gateways, set top boxes or modems) which execute software. These devices often contain sophisticated and secure application software, for example, software to decode and process signals (e.g., at the user's location) in order to provide specific content or services to the user. It may be desirable to change the software code images executing at the user's locations in order to update the software, provide new services, and enhance existing services, etc. However, downloading secure software from a central facility to devices in the field presents risks, such as the risk of unauthorized code being loaded onto a device. For example, malicious users may attempt to load an authenticated secure application code image intended for one device onto other similar devices that should not receive the code image. Other malicious users may attempt to load a previous application code image onto a device in order to exploit known bugs in the previous software version. The complexity of securely downloading software is further compounded by the large number of devices that may be involved, and the different content and services that may be provided to each device.

SUMMARY

The following presents a simplified summary of the disclosure in order to provide a basic understanding of some aspects. It is not intended to identify key or critical elements of the disclosure or to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the more detailed description provided below.

Some features described herein relate generally to providing a software download to a secure processor or other computing device. In some embodiments, a server or other computing device may generate an encryption key based on personalized unit data associated with the secure processor. The secure processor may generate a decryption key based on its own similar personalized unit data. A software download may be performed between the server and the secure processor in which an encrypted software code image is transmitted to the secure processor. The secure processor may then decrypt and load the software code image for execution.

Some additional features described herein relate to generating encryption and/or decryption keys for software downloads to one or more secure processors or other computing devices. In some embodiments, a software provider (e.g., a server) and/or a recipient device (e.g., a secure processor) may determine a sequence number or other data indicating one or more previous software downloads to a secure processor. Encryption and/or decryption keys for a software download may be generated based on personalized unit data including the determined sequence number or other data. In certain embodiments, sequences of multiple encryption and/or decryption keys may be generated to support multiple software downloads to a secure processor.

Other embodiments can be partially or wholly implemented on a computer-readable medium, for example, by storing computer-executable instructions or modules, or by utilizing computer-readable data structures.

The methods and systems of the above-referenced embodiments may also include other additional elements, steps, computer-executable instructions, or computer-readable data structures. In this regard, other embodiments are disclosed and claimed herein as well. The details of these and other embodiments are set forth in the accompanying drawings and the description below. Other features and advantages of the disclosure will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements.

FIG. **1** shows a high-level diagram of a computing device in communication with a plurality of secure devices in accordance with various aspects of the disclosure.

FIG. **2** illustrates some of the general elements of a computing device and a secure device in accordance with various aspects of the disclosure.

FIG. **3** shows a flow diagram of a process for transmitting encrypted software data to a secure device in accordance with various aspects of the disclosure.

FIG. **4** shows a flow diagram of a process for receiving and loading data onto a secure device in accordance with various aspects of the disclosure.

FIG. **5** illustrates a computing device providing data to a plurality of secure devices in accordance with various aspects of the disclosure.

FIGS. **6**A and **6**B illustrate a computing device providing data to a secure device multiple times in accordance with various aspects of the disclosure.

FIG. **7** shows a flow diagram of a process for generating a sequence of encryption and decryption keys in accordance with various aspects of the disclosure.

FIG. **8** shows a flow diagram of a process for transmitting an encrypted software code image to a plurality of secure devices in accordance with various aspects of the disclosure.

DETAILED DESCRIPTION

In the following description of the various embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown by way of illustration various embodiments in which aspects may be practiced. It is to be understood that other embodiments may be utilized and structural and functional modifications may be made without departing from the scope of the present disclosure.

FIG. **1** illustrates an example of a data distribution network on which many of the various features described herein may be implemented. In this example, a computing device such as control server **100** is configured to communicate with a plurality of secure devices, such as secure processors **200***a*-**200***n* over a communication network **300**. The control server **100** (or another computing device) may include one or more computing devices (e.g., network servers, personal computers, laptops, wireless devices, etc.) that may be configured to perform various functions and transmit various types of software and other data to the secure processors **200***a*-**200***n*. For example, the control server **100** may include a push notification server configured to generate push notifications to deliver data and/or commands to the secure processors **200***a*-**200***n*. The control server **100** may also include a content server configured to provide content to users based on software, instructions, and commands provided to the secure proces-